Lámpsakos | Nº. 8 | PP. 65 - 71 | julio-diciembre | 2012 | ISSN: 2145-4086 | Medellín - Colombia

LA INTERCEPTACIÓN DE DATOS INFORMÁTICOS ENTRE LA LICITUD Y LO DELICTUAL

DATA INTERCEPTION RECORDS BETWEEN LAWFULNESS AND DELICT

Esp. Ana María Mesa Elneser
Fundación Universitaria Luis Amigó
Medellín, Colombia

Esp. Jorge Eduardo Vásquez Santamaría
Corporación Universitaria de Colombia – IDEAS
Medellín, Colombia

(Recibido el 18/02/2012. Aprobado el 19/03/2012)

Resumen. El trabajo tiene como objeto hacer una reflexión sobre el límite legal e ilegal en actividades de interceptación de datos informáticos, resultado de la investigación interinstitucional en el campo probatorio en interrelación con la comisión de delitos informáticos proferidos mediante la Ley 1273 de 2009 en Colombia, el artículo expone los resultados alcanzados en torno a la presentación del delito consagrado en el artículo 269 C como parte del escenario necesario para comprender el alcance conductual y la consecuencia jurídica en tipos penales con doble regulación, esto es, campo físico tradicional y campo digital, que son los que demandan la existencia de una evidencia digital y facilitan su soporte probatorio. Finalmente cabe resaltar que el trabajo metodológico aplicado en la investigación fue dado con la técnica de rastreo documental, fichaje y análisis hermenéutico de la norma en correlación con la doctrina generalmente aceptada como fuente material de derecho, de ello se derivó el presente escrito en el cual se contiene solo una de las figuras legales investigadas durante el proyecto de investigación interinstitucional dado a instancias de la universidad EAFIT, Fundación Universitaria Luis Amigó y Fundación Universitaria de Colombia IDEAS en el año 2011 y parcial del 2012.

Palabras clave: Informática; Delito; Interceptación; Dato informático; Sistema informático; Orden judicial.

Abstract. With the overall aim of making a reflection on the legal limit and illegal activities Interception of computer data, resulting from research agency in the field of evidence developed in interaction with the computer crimes law proffered by 1273 of 2009 in Colombia the article presents the results obtained about the presentation of the crime of computer data interception as part of the stage necessary for understanding the scope behavioral and legal consequence criminal offenses dual regulation, ie traditional physical field digital field , the latter being those who demand the existence of digital evidence, in any case allowing his supporting evidence. Finally it should be noted that the work methodology applied in the research was given to the documentary screening technique, signing and hermeneutic analysis of the standard correlation with generally accepted doctrine as a material source of law, it was derived in the present paper which it contains only one of the legal concepts investigated during the research project agency given instances EAFIT university, Fundación Universitaria Luis Amigo IDEAS and Corporation Colombia university in 2011 and part of 2012.

Keywords: computer crime, interception, computer data, computer system, court order.

1. INTRODUCCIÓN

La presentación del tipo penal de interceptación de datos informáticos dispuesto en el artículo 269C de la Ley 1273 de 2009 o de delitos informáticos, es resultado del objetivo específico dirigido a la presentación de aquellos tipos penales a partir de las normas dispuestas con la Ley 1273 en Colombia, así como de legislación complementaria que resulta de estudios de casos de experiencias legislativas en el Derecho comparado.

Dicho objetivo encabeza los propósitos específicos del proyecto de investigación "*Informática forense y su aplicación en la investigación de los delitos informáticos consagrados en la Ley 1273 de 2009*" que propone como pregunta problema: ¿Se hace necesaria en Colombia la evaluación, identificación y determinación de las técnicas forenses en la investigación de delitos informáticos consagrados en la Ley 1273 de 2009?

2. DESARROLLO DEL ARTÍCULO

2.1 Los delitos informáticos

A partir del rastreo bibliográfico y la sistematización de información por medio de fichas, se pudo evidenciar un debate amplio y enriquecedor en torno a los denominados delitos informáticos. Entre las múltiples definiciones ofrecidas por la doctrina especializada se encuentra la del juez colombiano Alexander Díaz García [1], quien manifiesta que son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinada a producir un perjuicio a la víctima, atentados a la sana técnica informática, lo que, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actué con o sin ánimo de lucro (2011).

Por su parte, Cristian Andrés Meneses [2], citando a Julio Téllez Valdés, argumenta que los delitos informáticos se pueden conceptualizar de forma típica y atípica, entendiendo por la primera "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" [2]. Cristian Andrés Meneses cita también a Marcelo Huerta y Claudio Líbano [3], quienes expresan que estos delitos son:

> (…) aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.

A su vez, el profesor Téllez Valdés acude a la explicación del delito informático según Davara Rodríguez, quien lo define como la "realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software" [4].

El enriquecido debate da cuenta de una elaboración conceptual tan nutrida y variable como la tecnología misma y sirve de sustento a la figura de los delitos informáticos. En palabras de Carlos María Romeo Casabona citado por (PINO S. A.) se definía la realidad de los delitos informáticos desde la experiencia española en la década de los años ochenta de la siguiente manera:

> En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia

vinculada al computador o a las tecnologías de la información.

Vincular esta modalidad delictual exclusivamente a las computadoras está revaluado desde los alcances conceptuales de la informática jurídica, pues la especialización en la materia, como ha sucedido en el caso colombiano, ha identificado una variedad de elementos a partir de los cuales se configura la comisión de una variada gama de conductas tipificadas como delitos informáticos, como es el caso de los datos informáticos, un sistema informático o una red de telecomunicaciones.

Ello conduce a reiterar que la figura del delito informático no se refiere sólo a una modalidad de tipo penal sino a una multiplicidad de comportamientos que pueden y deben ser tipificados de forma independiente, claridad que aunque obvia, ha tenido fuerza en los aportes doctrinarios sobre la materia. En ello coinciden Acurio del Pino [4] y Romeo Casabona, quienes son enfáticos en reiterar que el delito informático alude a una pluralidad de conductas que incurren en la acción ilícita desde diversos elementos informáticos.

En tan amplio y dinámico debate se hace necesario contribuir y fortalecer la orientación conceptual de la figura del delito informático, especialmente para Colombia, por lo que se propone como definición de dicha modalidad delictual la referente a una conducta típica, antijurídica y culpable, de modalidad dolosa y no querellables, donde un sujeto despliega un comportamiento que se vale de un soporte tangible o intangible como datos informáticos, un sistema informático, red de telecomunicaciones o un soporte informático similar y atenta contra derechos de naturaleza fundamental como la intimidad y la información.

Como asegura Heidy Balanta [5] ningún organismo se ha atrevido a dar una definición concreta que integre todos los elementos de un delito informático, pues en ese intento se puede correr el riesgo de no incluir elementos propios de este delito, o confundirlo y caer en otro delito que no es el informático, adicional a los intensos cambios y variaciones de los soportes tecnológicos que sirven de elementos objetivos para que se configuren.

2.2 Interceptación de datos informáticos

> Artículo 269C: *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

La interceptación de datos informáticos es un delito penal básico o fundamental de conducta instantánea sin que pueda ser confundida como permanente, en la medida en que la conducta individualizada puede permanecer en el tiempo pero como un acto individualizado que se reitera paulatinamente frente a un sistema informático o las emisiones electromagnéticas, pero basta con una sola interceptación para conducir a su configuración típica.

Es un tipo penal simple por acarrear sólo una conducta como acción tipificada en la norma, y de aparente sujeto activo simple, en la medida en que, si bien la disposición comienza con "*El que*" sin que denote calidad especial alguna del sujeto que incurre en la conducta tipificada, la misma norma se encarga de condicionar la calidad especial del sujeto activo pensado para el tipo penal. Por lo tanto, este artículo conduce a que el sujeto activo de la interceptación debe ser un funcionario de la Policía judicial encargado de labores de investigación judicial en un proceso penal y que, para su legal ejercicio, requiere de orden judicial previa para realizar las interceptaciones a los medios señalados, circunstancia que requiere ahondar en las normas.

Tan delicada actividad tiene ampliamente desarrollada en la legislación nacional, puntualmente en la ya citada ley 906 de 2004, que especifica incluso que es deber de la Fiscalía General de la Nación "*informar a la autoridad competente de cualquier irregularidad que observe en el transcurso de la actuación de los funcionarios que ejercen atribuciones de policía judicial*" (Artículo 142, Ley 906 de 2004) lo que desde ahora implica asegurar que el sujeto activo de la acción citada en la interceptación de datos informáticos no es ni puede ser un sujeto común, debe ser un sujeto altamente cualificado que acredite los conocimientos suficientes para desplegar la acción en comento.

A partir del artículo 200 de la Ley 906 de 2004 se describe cuáles son los órganos de indagación e investigación penal en Colombia, por lo tanto, los facultados para llegar a proceder con una interceptación de datos informáticos. Cita el artículo 200:

> En desarrollo de la función prevista en el inciso anterior a la Fiscalía General de la Nación, por

conducto del fiscal director de la investigación, le corresponde la dirección, coordinación, control jurídico y verificación técnico-científica de las actividades que desarrolle la policía judicial, en los términos previstos en este código.

Señala la misma ley en su artículo 201 que ejercen permanentemente las funciones de Policía judicial los servidores investidos de esa función, pertenecientes al Cuerpo Técnico de Investigación de la Fiscalía General de la Nación, a la Policía Nacional y al Departamento Administrativo de Seguridad, por intermedio de sus dependencias especializadas.

También desempeñan funciones permanentes de Policía judicial de manera especial dentro de su ámbito de competencia las autoridades mencionadas en el artículo 202: Procuraduría General de la Nación, la Contraloría General de la República, las autoridades de Tránsito, las entidades públicas que ejerzan funciones de vigilancia y control, los directores nacional y regional del Inpec, los directores de los establecimientos de reclusión y el personal de custodia y vigilancia, conforme con lo señalado en el Código penitenciario y carcelario, los alcaldes y los inspectores de Policía.

Finalmente, el artículo 203 señala que ejercen funciones de Policía judicial, de manera transitoria, los entes públicos que, por resolución del Fiscal General de la Nación, hayan sido autorizados para ello. Estos deberán actuar conforme con las autorizaciones otorgadas y en los asuntos que hayan sido señalados en la respectiva resolución.

El Código de Procedimiento Penal dispuso en sus artículos 213 a 245 las actuaciones que no requieren autorización judicial previa para su realización por parte de las entidades que cumplen las funciones de Policía judicial.

La ley consagra como objetos amparados en la restricción de registro por parte de las autoridades que adelantan la investigación, los siguientes:

No serán susceptibles de registro los siguientes objetos:

1. Las comunicaciones escritas entre el indiciado, imputado o acusado con sus abogados.
2. Las comunicaciones escritas entre el indiciado, imputado o acusado con las personas que por razón legal están excluidas del deber de testificar.
3. Los archivos de las personas indicadas en los numerales precedentes que contengan información confidencial relativa al indiciado, imputado o acusado**. Este apartado cobija también los documentos digitales, videos, grabaciones, ilustraciones y cualquier otra imagen que sea relevante a los fines de la restricción.**

PARÁGRAFO. Estas restricciones no son aplicables cuando el privilegio desaparece, ya sea por su renuncia o por tratarse de personas vinculadas como auxiliadores, partícipes o coautoras del delito investigado o de uno conexo o que se encuentre en curso, o se trate de situaciones que constituyan una obstrucción a la justicia. (Negrilla fuera de texto original).

A partir de las disposiciones citadas, la Fiscalía encuentra como limitante en la actividad investigativa la posibilidad de acceder a los datos de información contenidos en sistemas o soportes informáticos, restricción que inicialmente impide que en un registro o allanamiento ordenado o autorizado por Fiscalía, se tenga acceso a los datos informáticos, situación que se rompe en las circunstancias descritas en el parágrafo del artículo 223 de la Ley 906 de 2004.

La ley 906 detalla entre las actividades y elementos que pueden ser objeto de investigación sin autorización previa de un juez, comprendido en el artículo 235 modificado por el artículo 52 de la Ley 1453 de 2011 que dispone:

Interceptación de comunicaciones. El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se **intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación.** En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación así como del procesamiento de la misma. **Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación**.

En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva.

Por ningún motivo se podrán interceptar las comunicaciones del defensor.

La orden tendrá una vigencia máxima de seis (6) meses, pero podrá prorrogarse, a juicio del fiscal, subsisten los motivos fundados que la originaron.

La orden del fiscal de prorrogar la interceptación de comunicaciones y similares deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías. (Negrilla fuera de texto original).

Es esta disposición la que acarrea el pronunciamiento de la Corte Constitucional y la consiguiente exigencia de orden judicial para adelantar la interceptación de datos informáticos como medio de comunicación. Al respecto, señaló la Corporación en sentencia C – 334 de 2010:

> Con la modificación introducida al artículo 250 constitucional por el Acto Legislativo No. 3 de 2002, se contemplan, en términos generales, tres tipos de intervención por parte de la Fiscalía. Una primera, la habilitación legal para "realizar excepcionalmente capturas", la cual se somete, al tenor del numeral 1º, a un control de legalidad posterior dentro de las 36 horas siguientes a la práctica de la medida; **otra, en la cual se contemplan los "registros, allanamientos, incautaciones e interceptaciones de comunicaciones", que también, conforme al inciso 2º, son controlados con posterioridad a su práctica y dentro de las 36 horas siguientes;** y finalmente, las demás "medidas adicionales que impliquen afectación de derechos fundamentales", previstas en el numeral 3º, las que sí requieren "autorización por parte del juez que ejerza las funciones de control de garantías para poder proceder a ello", con lo que se quiere significar que, salvo la práctica de exámenes sobre la víctima de delitos o agresiones sexuales, las intervenciones de la Fiscalía que requieren autorización judicial, operan sobre la persona contra quien cursa la investigación. (Negrilla fuera de texto original).

En la citada sentencia de la Corte Constitucional, la interceptación de comunicaciones requiere de control judicial "posterior", diferente a la mencionada orden judicial "previa" dispuesta en la norma del tipo penal de interceptación de datos informáticos.

Queda así por vía de interpretación jurisprudencial despejado el alcance de la acción a la que alude la interceptación tipificada en el artículo 269C, y complementa la interpretación del Tribunal los alcances también dispuestos por la norma en relación con los tipos de violación del bien jurídicamente tutelado, en la medida en que el tipo penal se refiere al origen, destino o interior de un medio informático, lo que se traduce en la movilidad posible de los datos informáticos entre los usuarios de un sistema informático, asunto al que se refirió la Corte en los siguientes términos:

> En esa oportunidad también se indicó que ese tipo de violaciones *"pueden suceder bien por examinarla persona que no sea el destinatario o alguien a quien éste la muestre, en cualquiera de los momentos anotados, es decir, su elaboración,* ***curso del traslado o después de recibida;*** *bien con violencia o habilidad en la extracción y examen de su contenido; bien con destrucción del objeto portador de la información, quitándole alguna parte o tornándolo ininteligible"*. (Negrilla fuera de texto original).

Seguidamente, en la misma sentencia la Corte Constitucional retoma el mandato legal del control judicial posterior que debe cumplir la Fiscalía en los casos de haber ordenado interceptación de comunicaciones en la etapa de investigación de un proceso penal. En ella se reitera:

> Sin embargo, el legislador en materia penal al regular el tema ha señalado que el Fiscal puede ordenar, fundadamente y por escrito, la **interceptación** *"mediante grabación magnetofónica o similares las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético"*, para buscar elementos materiales probatorios y evidencia física, para la búsqueda y ubicación de imputados o indiciados, **debiendo comparecer ante el Juez de Garantías dentro de las 24 horas siguientes al diligenciamiento de la orden, para que se realice la revisión de la legalidad de lo actuado, así como dentro de igual término una vez cumplida la misión, para que se adelante el mismo control** (arts. 235 a 237 L. 906 de 2004 conc. L. 1142 de 2007). (Negrilla fuera de texto original).

La Corte Constitucional fortaleció las medidas de protección y garantía de los derechos fundamentales que se relacionan con la actividad de investiga-

ción penal que adelantan las autoridades de la Policía judicial en Colombia. Sin excluir la regla general del control judicial posterior que exige la ley 906 de 2004, estimó la Corte que la interceptación de comunicaciones cuando especifica textualmente la inclusión de los archivos digitales y documentos computarizados que requieren de la previa autorización del juez para adelantar la diligencia, todo en virtud de la protección del derecho fundamental de la intimidad y la hace, para el caso de las interceptaciones, regla general de procedimiento.

> La Corte Constitucional en la sentencia C-336 de 2007 puntualizó que **la exigencia de ese control previo, como regla general, deviene del fortalecimiento que se da en el sistema acusatorio de investigación penal al principio de reserva judicial, cuando de la afectación de derechos fundamentales se trate** (reitera lo expuesto en la C-1092 de 2003, ya referida, donde se declaró inexequible la expresión *"al solo efecto de determinar su validez"*, del numeral 2° del artículo 2° del Acto Legislativo 03 de 2002 que modificó el artículo 250 superior). (Negrilla fuera de texto original).

De esa forma la interceptación de datos informáticos queda amparada por una doble garantía; inicialmente requiere de orden judicial previa en virtud de la naturaleza del derecho fundamental de intimidad que es puesto en observación de las autoridades de Policía judicial; y al control posterior que, por mandato de ley, debe cumplir el funcionario cuando realice la diligencia de interceptación.

A partir de la misma redacción del tipo penal en estudio, y de los amplios pronunciamientos jurisprudenciales generados en torno al tema, se estima necesario hacer una reflexión crítica y constructiva del tipo penal. Bien exige el artículo 269C para la configuración de la conducta punible la ausencia de orden judicial previa, condición necesaria para la interceptación de datos informáticos, contrario a lo perseguido por el ordenamiento jurídico, pero como se vio, la misma actuación también queda sujeta a un control judicial posterior que no figura como elemento del tipo penal.

Desde el campo informático con alcance del ámbito jurídico es necesario establecer alcance terminológico del tipo penal del artículo 269C denominado De la *Interceptación de datos informáticos.*

Se habla de la existencia de orden judicial para interceptar datos informáticos, es decir, la aplicación del término *interceptar* referido a extraer datos que están en un proceso de movimiento cuando se identifica con acciones de envió, recepción, transferencia, y se excluyen los datos estáticos de su consagración.

Igualmente, se describe que los datos objeto de interceptación pueden ser los datos en su origen (es decir, el punto donde se envía), en su destino (es decir, al punto donde llega) o en el interior de un sistema informático (hay que aclarar el concepto sistema informático) pero no especifica en intermedio del receptor y el emisor (si es que es posible).

También alude de las emisiones electromagnéticas provenientes de un sistema informático, puesto que hay muchas formas de comunicación por medio de emisiones electromagnéticas (entre ellas está la radio, el wifi, los celulares, entre otros), comunicaciones que pueden ser interceptadas que se hacen pasar por el receptor. Si se refieren a un sistema informático también se incluye la intercepción de información entre la persona y el dispositivo informático que se incluya en el sistema de información.

4. CONCLUSIONES

- La implementación de la TI dedicada a la transferencia de comunicaciones P2P, siempre tendrá una tendencia de vulneración a la intimidad de comunicaciones, por lo cual los datos informáticos se convierten en el objetivo principal de realización de conductas delictivas de forma involuntaria en la utilización de mecanismos tecnológicos informáticos tipo software. Entre otros, encontramos los Keylogger instalados en los equipos del mismo usuario, debido a la captura de datos informáticos en el momento de su transferencia.
- El tipo penal de interceptación, por requerir aspectos objetivos que validan su ejecución como son la orden judicial y el control ante el juez con función de control y garantías, establece la línea divisoria entre las conductas constitutivas de licitud o ilicitud al desplegarse una actividad de interceptación, por cuanto estos dos requisitos formales y materiales requieren conocimiento y materialización, para que produzca efectos jurídicos vinculantes, es decir, para evidenciar el estado de conciencia en el momento de la realización de la conduc-

ta. Se deja por fuera la judicialización de personas calificadas dentro del grupo de delincuentes o atacantes informáticos como Lamers y Copyhackers, donde se creería la inexistencia de intencionalidad dolosa, desde un punto de vista jurídico, no así desde un ámbito informático, el cual, claramente no se encuentra enmarcado en nuestro ordenamiento jurídico en el momento de incluir las modalidades de participación autoral en la comisión de delitos.

AGRADECIMIENTOS

Los autores reconocen las contribuciones y el apoyo institucional que las IES Fundación Universitaria Luis Amigó, Eafit e Ideas, sede Itagüí, tuvieron al cofinanciar el proyecto ejecutado en el año 2011, que generó un avance académico investigativo no sólo para el conocimiento de la comunidad académica de cada una, sino, también, del contexto social colombiano, que se evidencia con la multiplicidad de participación en eventos de divulgación en cuanto a los resultados obtenidos, tal como se advierte en el presente artículo.

REFERENCIAS

[1] Díaz García, A. (2010). *Aniversario en Colombia del nuevo delito de violación de datos personales. Primer año de vigencia de la Ley de Delitos Informáticos*. Recuperado de http://alejandrodelgadomoreno.com/2010/01/aniversario-de-la-ley-de-delitos.html

[2] Meneses, C. A. (2002). *Delitos Informáticos y nuevas formas de resolución del conflicto penal chileno*. Recuperado de http://www.delitosinformaticos.com/delitos/penalchileno.shtml

[3] Huerta, M. & Líbano, C. (S. A.). Los delitos informáticos. En: Acurio del Pino, S. (Ed). *Delitos informáticos: generalidades.* Editorial Jurídica Cono Sur. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[4] Acurio del Pino, S. *Delitos informáticos: Generalidades.* Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf. Noviembre 2011.

[5] Balanta, H. (2009). *Aproximación legal a los delitos informáticos: una visión de derecho comparado*. Cali: Ponencia presentada en el II Congreso Internacional de Criminología y Derecho Penal.

Legislation (Legislación) Ley 599 de 2000, por medio de la cual se expide el Código Penal de Colombia.
Ley 906 de 2004, por medio de la cual se expide el Código de Procedimiento Penal.
Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1288 de 2009, por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones.

Jurisprudence (Jurisprudencia)
Corte Constitucional de Colombia, 2007. Sentencia C – 336, M.P.: Jaime Córdoba Triviño.
Corte Constitucional de Colombia, 2009. Sentencia C – 025, M.P.: Rodrigo Escobar Gil.
Corte Constitucional de Colombia, 2010. Sentencia C – 334, M.P.: Juan Carlos Henao Pérez.
Corte Constitucional de Colombia, 2009. Sentencia C – 131, M.P.: Nilson Pinilla Pinilla.